UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/664,919	09/18/2000	Jeffrey M. Drew	NAI1P194/99.115.01	4381

28875 7590 06/04/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	7

DATE MAILED: 06/04/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/664,919	DREW, JEFFREY M.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *6* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 3/15/2004, applicant amends claims 1, 5, 7, 8, 9, 12, and adds claim 15. The following **claims 1-15** are presented for examination.

2. The amendments to the specification, pages 2-3, filed on 3/15/2004 have been considered. The objection to claim 5 has been withdrawn. The rejection to claims 9-12 under 35 USC 101 has been withdrawn.

2.1 Applicant's arguments, pages 10-13, filed on 3/24/2004, with respect to the rejection of claims 1-8 have been fully considered, but are not persuasive. Applicant amended at least the independent claims and upon further consideration of the new claim limitations as amended, a new ground of rejection is made in view of Branham. Branham teaches at least the new limitations of the amended claims. Therefore the claims are rejected in view of Branham in combination with the previous references. Applicant argues that the elements are not arranged as claims. Examiner is making clear the distinction between the prior art figures 1-2 and the claimed invention in previous Office Action and this Office Action by clearly showing the difference between the claimed invention and the prior art figure disclosure by Applicant. For instance, Applicant admitted that prior art figure teaches detecting a request for closure of an opened computer file, and also discloses scanning said opened file for virus before closure. Prior art also teaches closing said file after scanning for viruses if found virus free. The difference

between claim 1 and the prior art is determining if file has been modified since being opened before closure in response to and after a closure request; and closing said file if unmodified. Branham also discloses determining in response to and after a closure request, but before file closure if an opened file has been modified since being opened, which is typically determining if file has been modified in response to and after a write request but before writing to disk. Branham further discloses closing said file if unmodified and closing said file after scanning for viruses if found virus free. Applicant also admitted that it is known in the art operating system to store files upon opening in unmodified state.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-4, 6-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,398,196 to **Chambers** in view of International Application Publication WO-93/25024 (PCT/US93/05029) to **Branham** and in view of AAPA (Applicant Admitted Prior Art).

3.2 **As per claims 1 and 6, Chambers** substantially teaches a method for optimizing the operation of an anti-virus computer program for use with an operating system, comprising the steps of: detecting a request for closure of an opened computer file and determining in response to a closure if the opened computer file has been modified since being opened, for example (see column 10, lines 7-14). **Chambers** does not explicitly disclose the step of determining in response to and after a closure request, but before file closure if an opened file has been modified since being opened. It is known in the art as Applicant Admitted Prior Art discloses that an opened file is scanned for viruses before closure. **Branham** in an analogous art teaches using a networking environment the step of determining in response to and after a closure request, but before file closure if an executable file has been modified that meets the recitation of if an opened file has been modified since being opened in order to ensure that executable files should never be altered and to destroy the virus which caused the change, for example (see page 6, line 16 through page 7, line 15 and page 8, line 4 through page 8, line 27; page 3, lines 15-26; page 5, lines 20-32). Even though **Branham** refers to executable files with (.exe, .com and the like), it is well known to one skilled in the art that the executable file can be an opened executable file without departing from the spirit and scope of the invention disclosed by **Branham**. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Chambers** to determine in response to and after a closure request, but before file closure if an opened file has been modified since being opened as taught by **Branham** in order to detect when a file is altered and to destroy the virus which caused the change (see page 3, lines 15-26; page 5, lines 20-32). This modification would have been obvious because

one skilled in the art would have been motivated by the suggestions provided by **Branham** so as to detect when a file is altered and to destroy the virus, which caused the change.

Chambers discloses scanning a file if file has been modified, but **Chambers** does not explicitly disclose scanning said opened file for viruses before closure only if said opened file has been modified and closing said file if unmodified, and closing said file after scanning for viruses if found virus free. It is known in the art as Applicant Admitted Prior Art discloses that an opened file is scanned for viruses before closure and closing said file after scanning for viruses if found virus free (see prior art figure 2 and description). **Branham** in an analogous art teaches the step of scanning said opened file for viruses before closure only if said opened file has been modified and closing said file if unmodified, and closing said file after scanning for viruses if found virus free, for example (see page 6, line 16 through page 7, line 15 and page 8, line 4 through page 8, line 27; page 3, lines 15-26; page 5, lines 20-32). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Chambers** to scanning said opened file for viruses before closure only if said opened file has been modified and closing said file if unmodified, and closing said file after scanning for viruses if found virus free as taught by **Branham** in order to detect when a file is altered and to destroy the virus which caused the change (see page 3, lines 15-26; page 5, lines 20-32). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Branham** so as to detect when a file is altered and to destroy the virus, which caused the change.

As per claim 2, Chambers discloses the limitation of determining whether said operating system includes a "dirty cache buffer" to raise or set a modification flag relative to a file being modified during the time it has been open, a computer code being indicative of said flag, and using the computer code for a raised or set modification flag, if available, for carrying out said modification determining step by checking for the presence of a raised modification for said file, for example (see column 10, lines 7-14 and see column 9, lines 11-60).

As per claim 3, Chambers discloses the limitation of if it's determining that said operating system does not provide a modification flag, said method further includes the steps of establishing a "dirty cache buffer" to raise a modification flag if and opened file associated with said flag has being modified by a write operation, for example (see column 3, line 64 through column 4, line 3). **Chambers** discloses that the program also has means of executing the steps of the above claim 2 on its own.

As per claim 4, Chambers discloses the limitation of wherein said operating system includes a "dirty cache buffer for providing a computer code for a modification flag indicative of the modification of an open file, said method further including in said modification determining step of detecting the presence of said modification flag to determine if the associated file has been modified, for example (see column 10, lines 7-14 and see column 9, lines 11-60).

As per claim 7, Chambers substantially teaches a method for optimizing the operation of an anti-virus program in an operating system, said operating system including programming

for raising a flag indicative of modification of an open file during the time the file has been open said method including the steps of detecting the event of a request for closing said file being made to said operating system; determining whether said modification flag has been raised by said operating system for said file (see column 10, lines 7-14 and see column 9, lines 11-60). Prior art discloses scanning an opened file for virus before file closure. **Chambers** does not explicitly disclose the step of detecting the event of a request for closing said file after said detecting but before file closure. **Branham** in an analogous art teaches the step of determining whether said modification has flag has been raised by said operating system for an executable file, for example (see page 2, lines 1-15). **Branham** further discloses scanning said open file in response to said modification flag, for permitting said operating system to close said file; and skipping said step of scanning for viruses before closure of said open file whenever said modification flag is not present, for example (see page 6, line 16 through page 7, line 15 and page 8, line 4 through page 8, line 27; page 3, lines 15-26; page 5, lines 20-32).. These limitations are similar to the limitations found in the rejected claim 1 except for using a modification flag. Therefore **claim 7** is rejected on the same rationale as the rejection of **claim 1**.

Claim 8 is similar to claims 5 and 7. Therefore, claim 8 is rejected on the same rationale as the rejection of claims 5 and 7.

4. **Claims 9-14** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,319,776 to **Hile et al.** in view of International Application Publication WO-93/25024 (PCT/US93/05029) to **Branham** and in view of AAPA (Applicant Admitted Prior Art).

4.1 **As per claim 9, Hile et al.** substantially teaches a computer program for detecting computer viruses on a file server, the file server providing file storage and retrieval services for at least one client computer over a network, said computer program product comprising: computer code for detecting an open request from a client computer, the open request asking for a requested file from the server, for example (see column 6, lines 5-39); computer code for scanning said requested file for computer viruses, whereby the file server is permitted to provide said requested file to the client computer if no computer viruses are found therein, for example (see column 6, line 66 through column 7, line 6); computer code for detecting a close request from the client computer associated with said requested file, for example (see column 7, lines 23-24); scanning said requested file for computer viruses if said requested file was changed prior to said close request, for example (see column 7, lines 24-27). **Hile et al.** does not explicitly disclose the step of for skipping scanning said requested file if it was not changed prior to said close request. **Branham** in an analogous art teaches the step of after said detecting, but before file closure, accessing an operating system flag that indicates whether the requested file was changed prior to said close request; scanning said requested file for computer viruses if said requested file was changed prior to said close request; and skipping scanning said requested file if it was not changed prior to said close request, for example (see page 6, line 16 through page 7, line 15 and page 8, line 4 through page 8, line 27; page 3, lines 15-26; page 5, lines 20-32).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of **Hile et al.** to include the step of after said detecting, but before file closure, for skipping scanning said requested file if it was not changed prior to said close request. as taught by **Branham** in order to detect when a file is altered and to destroy the virus which caused the change (see page 3, lines 15-26; page 5, lines 20-32). This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Branham** so as to know when a file is altered and to destroy the virus, which caused the change.

Claim 12 recites the same limitation as the rejected claim 9 except for the step of determining whether a virus vulnerable portion has been modified which is disclosed by **Branham**. Therefore, claim 12 is rejected on the same rationale as the rejection of claim 9.

As per claims 10 and 13, Hile et al. discloses the limitation of wherein said operating system flag is generated externally to said computer program product by the operating system in order to reduce redundant disk writes, whereby said computer code for scanning is invoked upon closing of the requested file only when actual disk writes are made by the operating system for the requested file, for example (see column 6, lines 28-39; see also figure 6a).

As per claims 11 and 14, Hile et al. discloses the limitation of wherein said computer code for accessing uses a file handle generated by the operating system to identify the operating

system flag corresponding to the requested file, said handle having been generated when the file was opened, for example (see column 6, lines 28-39; see also figure 6a).

5. **Claims 5 and 15** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 5,398,196 to **Chambers** in view of International Application Publication WO-93/25024 (PCT/US93/05029) to **Branham** and in view of AAPA (Applicant Admitted Prior Art) as applied to claims 1-4 above and further in view of US Patent 5,649,095 to **Cozza**.

5.1 **As per claim 5,** both references substantially teach the claimed method of claim 4. It is well known in the art program that discloses the step of scanning a file for viruses in response to a request for opening the file and opening the file if virus free, such steps are disclosed in US Patent 5,956,481, Walsh et al.. **Branham** discloses the step of indicating an open file is unmodified in the absence of an associated modification flag, for example (see page 2, lines 1-15). Both references do not explicitly disclose establishing a cache buffer memory for storing only a vulnerable portion. **Cozza** in an analogous art teaches the step of establishing a cache buffer memory for storing upon opening of a file only a virus vulnerable portion of that file that a virus must use to enter and infect said file; said modification determining step including the steps of indicating an open file is unmodified in the absence of an associated modification flag; responding to the presence of a modification flag by comparing a portion of said open file to the associated unmodified virus vulnerable portion of said file in said cache buffer memory to determine if the portion of the open file has been modified since the opening of the file

indicating the opened file is unmodified if the virus vulnerable portion is unmodified and modified if the portion is modified (see column 6, lines 21-45). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method as combine above to store and compare only a virus vulnerable portion of said file as taught by **Cozza** to guarantee a great scanning speed increase. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Cozza** so as to guarantee a great scanning speed increase.

5.2 **Claim 15** recites the same limitations found in the rejected **claims 1, 4, and 5**. Therefore, **claim 15** is rejected on the same rationale as the rejection of **claims 1, 4, and 5**.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 703-305-0355. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

cc

Carl Colin

Patent Examiner

May 28, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100